Michigan State Police

LEIN Audit and Training Unit

Audit Process

April 12, 2013

Outline

I. LEIN Audit Process

II. Technical Security Review

A Closer Look…

III. Audit Review

IV. Common Findings

LEIN Audit Process

LEIN Audit Process

Why we audit:

- Congressionally-mandated program established by the FBI in 1983
- FBI CJIS Security Policy requires CJIS Systems Agency (CSA) to audit local agencies
- Objective is to evaluate/ensure users are properly following guidelines set forth in the FBI’s CJIS Security Policies
- Maintain and enhance Officer/Public Safety

LEIN Audit Process

Who gets audited:

- Any agency with direct access to LEIN; criminal justice agencies, non-criminal justice agencies, agencies with MDT/MCT only access

  - Law Enforcement Agencies
  - Department of Corrections
  - Courts (criminal divisions)
  - Probation and Parole
  - Prosecuting Attorneys
  - Public Safety Agencies
  - Central Dispatch Centers

LEIN Audit Process

Who gets audited:

- Types of Access
  - Direct Access Agency
  - Interface Agency
  - Interface Provider Agency
  - Interface Subscriber Agency
  - MiCJIN Token Agency

LEIN Audit Process

- Direct Access Agency
  - Accesses LEIN via the MiCJIN Portal with Mnemonic (includes SOR and APRS)

- Interface Provider Agency
  - Holds a POP/Server connecting to LEIN
  - May provide access to other agencies
  - Devices accessing LEIN – i.e. PC, MDT/MDC

LEIN Audit Process

- Interface Subscriber Agency

  - Connects to LEIN via an Interface Provider

  - Devices accessing LEIN – i.e., PC, MDT/MDC

- MiCJIN Token Agency

  - Connects to LEIN via the MiCJIN Portal over the public Internet using a token, no mnemonic (includes SOR and APRS)

LEIN Audit Process

How Often:

- Once in a three-year cycle
  - Currently in the 2010-2013 cycle
  - Current cycle ends June 30, 2013
- Audit Notification
  - 30 days prior by telephone
  - Mutual date and time
  - Discuss with TAC four areas of review and required documentation
  - Written notice to agency head, TAC, and LASO

LEIN Audit Process

Be Prepared!!

- Read the directions! Audit procedures may have changed since the last audit
- Call Auditor or LEIN Field Services with questions

Unprepared = Unsatisfactory rating

LEIN Audit Process

Areas of Review:

- **Administrative**
  - Operator Certification, Training/testing
  - LEIN User Agreement with MSP, Fire Dept./School agreements, etc.
  - Agency policies and procedures

- **Criminal History** (QLOG)
  - Written documentation to support 50 queries
  - Use of required fields: Purpose Code, Purpose Code Reason, OCA, Remarks, Requestor
  - Proper Access: C/, J/, M/, E/, F/, etc.

LEIN Audit Process

Areas of Review:

- **Data Quality** – agencies that own/enter records
  - Warrants
  - PPOs
  - Stolen Vehicles
  - Missing Persons

- Suggest use monthly validation listings to pull records
- Require agency to print requested records prior to audit
- "Auditable" fields are defined for record types; subject to change

LEIN Audit Process

Areas of Review:

- **Technical Security**
  - Review Technical Security Review Questionnaire
  - Site security
  - Approved current CJIS Network Diagram
  - Fingerprinting and background checks
  - Security Awareness Training
  - Required Security Policies/Procedures: Acceptable use including criminal penalties, Anti-virus software, Passwords, Unique Identifiers
  - System-enforced passwords; unique user names (no generics)
  - Media Disposal; Secondary Dissemination
  - Management Control Agreements with IT Contractors
  - CJIS Security Addendums (if applicable)

LEIN Audit Process

Rating Thresholds

Finding	Rating	Disposition
No errors, deficiencies or misuse	Satisfactory	Exceeds Standards
1-5% error per DQ category, minor deficiencies	Satisfactory	Meets Standards On-site training
5-10% error per DQ category, 1st time	Unsatisfactory	On-site training Written response
5-10% error per DQ category, 2nd time	Unsatisfactory	CSO Referral Written response
10% + error per DQ category	Unsatisfactory	Refer to CSO

LEIN Audit Process

Rating Thresholds

Finding	Rating	Disposition
Improper Use/Misuse	Unsatisfactory	CSO Referral
One or more undocumented CHR inquiries	Unsatisfactory	On-site training Written response
Average Time for Entry is greater than 72 hours	Unsatisfactory	On-site training Written response
Security Violation i.e., modifiable OPR field, sharing user name/token, non-compliant passwords	Unsatisfactory	CSO Referral

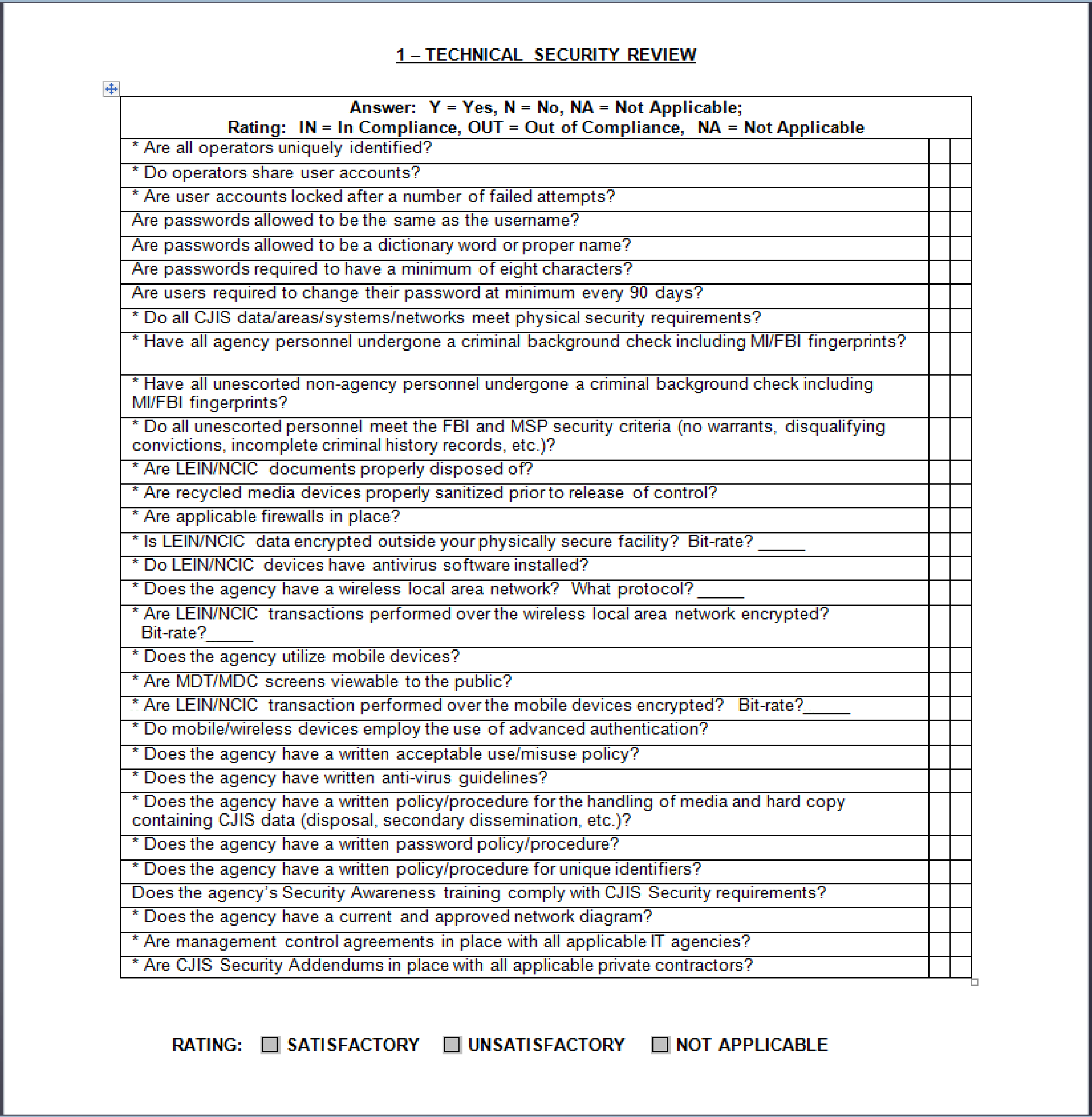
LEIN Audit Process

Overall audit rating is equal to the lowest individual area rating:

Technical Security	-	Satisfactory
Administrative	-	Satisfactory
CHR Review	-	Satisfactory
Data Quality	-	Unsatisfactory

Overall Audit Rating = Unsatisfactory

Technical Security Review A Closer Look…



1 – TECHNICAL SECURITY REVIEW

Answer: Y = Yes, N = No, NA = Not Applicable; **Rating: IN = In Compliance, OUT = Out of Compliance, NA = Not Applicable**		
* Are all operators uniquely identified?		
* Do operators share user accounts?		
* Are user accounts locked after a number of failed attempts?		
Are passwords allowed to be the same as the username?		
Are passwords allowed to be a dictionary word or proper name?		
Are passwords required to have a minimum of eight characters?		
Are users required to change their password at minimum every 90 days?		
* Do all CJIS data/areas/systems/networks meet physical security requirements?		
* Have all agency personnel undergone a criminal background check including MI/FBI fingerprints?		
* Have all unescorted non-agency personnel undergone a criminal background check including MI/FBI fingerprints?		
* Do all unescorted personnel meet the FBI and MSP security criteria (no warrants, disqualifying convictions, incomplete criminal history records, etc.)?		
* Are LEIN/NCIC documents properly disposed of?		
* Are recycled media devices properly sanitized prior to release of control?		
* Are applicable firewalls in place?		
* Is LEIN/NCIC data encrypted outside your physically secure facility? Bit-rate? _____		
* Do LEIN/NCIC devices have antivirus software installed?		
* Does the agency have a wireless local area network? What protocol? _____		
* Are LEIN/NCIC transactions performed over the wireless local area network encrypted? Bit-rate?_____		
* Does the agency utilize mobile devices?		
* Are MDT/MDC screens viewable to the public?		
* Are LEIN/NCIC transaction performed over the mobile devices encrypted? Bit-rate?_____		
* Do mobile/wireless devices employ the use of advanced authentication?		
* Does the agency have a written acceptable use/misuse policy?		
* Does the agency have written anti-virus guidelines?		
* Does the agency have a written policy/procedure for the handling of media and hard copy containing CJIS data (disposal, secondary dissemination, etc.)?		
* Does the agency have a written password policy/procedure?		
* Does the agency have a written policy/procedure for unique identifiers?		
Does the agency's Security Awareness training comply with CJIS Security requirements?		
* Does the agency have a current and approved network diagram?		
* Are management control agreements in place with all applicable IT agencies?		
* Are CJIS Security Addendums in place with all applicable private contractors?		

RATING: □ **SATISFACTORY** □ **UNSATISFACTORY** □ **NOT APPLICABLE**

…a closer look

- Technical and Physical Security

  - FBI CJIS Security Policy (current version v5.1)
  - Michigan CJIS Security Addendum

❖ Protection of Criminal Justice Information (CJI includes information obtained from LEIN/NCIC)

❖ All agencies with access to CJI must have a Local Agency Security Officer (LASO)

…a closer look

- TSR Questionnaire

  Questions pertaining to agency’s information systems, infrastructure and security

  - Provided to agency prior to audit (mailed audit packet)
  - Required to be completed by LASO prior to audit
  - Reviewed with LEIN TAC and LASO at audit
  - Questionnaire is one-size fits all (law, courts, corrections)
  - Becomes part of final report

...a closer look

- LASO (Local Area Security Officer)

  - Point of contact for network and security issues

  - Ensure compliance with FBI CJIS Security Policy/Michigan Addendum

  - Ensure proper technical and physical security measures in place

  - Maintain network diagram

  - Report non-compliance/violations

…a closer look

- LASO continued…

  - Conduct/document Security Awareness Training

  - Establish/maintain written policies/procedures

  - Maintain Management Control Agreements with non-CJ agencies (IT Dept, IT Contractor), including CJIS Security Addendums (as applicable)

  - Audit

…a closer look

- TSR Questionnaire Segments:
  - I. LEIN/NCIC System Administration
    - -Name(s) / Agency
  - II. Authentication and User Identification
    - -Unique identifiers, passwords
  - III. Physical Security
    - -Workstations, public access, equipment areas
  - IV. Personnel Security
    - -Fingerprinting / Background Checks
    - -Security Awareness Training
  - V. Media (hard copy/paper, diskette, tape, CD, hard drive, etc.)
    - -Storage / Disposal

...a closer look

- TSR Questionnaire Segments:

  VI. Backups

  -Secure location / inventory

  VII. Network Environment

  -Who manages, Management Control Agreement, CJIS Security Addendums, encryption, anti-virus, etc.

  VIII. Wireless

  -WLAN, mobile devices, AA, encryption

  IX. Dial up/Dial back Access

  -Who initiates / manages, AA

  X. Documentation (LEIN-specific)

...a closer look

- TSR Questionnaire Segments:

  X. Documentation (LEIN-specific)
  - Policies / Procedures:
    - Acceptable Use (standards of discipline)
    - Anti-Virus
    - Media and Hard Copy Handling (secondary dissemination)
    - Passwords
    - Unique Identifier

  - Training Log (Affirmation List)
  - Security Awareness Training
  - Network Diagram
  - Management Control Agreements
    - CJIS Security Addendums (if applicable)

…a closer look

- Management Control Agreements

  - **Government IT Departments** (non-CJ contractors)

    * Must sign a management control agreement ensuring CJ management control

  - **Private IT Contractors** (non-gov’t contractors)

    * Must sign a management control agreement defining scope of use/CJ management control

    * All contractor employees who access information must sign CJIS Security Addendums

...a closer look

- CJIS networks connected to the Internet must be protected by a firewall
- All CJI traveling outside the boundaries of a physically secure location must be encrypted at 128 bit
- CJI at rest outside a physically secure location must be encrypted at 128 bit
- All workstations/servers must have anti-virus software installed, regardless of Internet access
- Authentication
  - Users shall be uniquely identified
  - Password requirements

...a closer look

- Passwords must be:

  - System enforced
  - Kept secret
  - At least 8 characters
  - Not a dictionary word or name
  - Changed at a minimum every 90 days
  - Must not use last 10 passwords
  - Encrypted

…a closer look

- Advanced Authentication

  Provides for the additional security to the typical user ID and password

  - Used when accessing from outside a secure facility i.e., VPNs (IPSec), Biometrics, public key infrastructure, smart cards, software tokens, hardware tokens, or “risk-based authentication” (device forensics, challenge/response questions, etc.)

…a closer look

- Physical Security

  - Workstations/data/networks must be secured and unavailable to those who are not allowed access

  - Visitors to secured areas must be escorted at all times

  - Persons with unescorted access to secured areas, workstations/data/networks, must be fingerprinted and background checked (non-LEIN certified staff, IT personnel, janitorial/maintenance, city manager, etc.)

…a closer look

- LEIN Audit Process:
  - Facility walk-through conducted with TAC / LASO
    - Workstation/data viewable by public
    - Security of workstation/data
    - Equipment room locked, limited access
    - Shared space
  - Visual “spot check” of equipment room, location, security
  - Identify problems/issues/concerns with TAC/LASO
  - Document findings in audit report

Audit Review

- Review hot items/current trends, new/upcoming changes
- Hold individual agencies accountable for compliance with rules, policies and procedures
- Audit process, questions, format may change to reflect trends or issues
- Agencies are required to comply with entire FBI CJIS Security Policy and Michigan Addendum

Common Findings

Common Findings

- Courts and encryption
- System enforced password compliance
- Lack of fingerprinting/background checks – unescorted access to CJI (city managers, janitorial/maintenance personnel, etc.)
- Expansion of Security Awareness Training requirements – persons who access/receive CJI (prosecutors, court personnel, LE at non-term agencies, etc.)
- Technical Security required policies and procedures
- Provider/Subscriber may be compliant / other agencies may not be

Questions??

The End